SAP as CNA (CVE Numbering Authority) - All you need to know

Shipra Aggarwal
Security Response, Bangalore
SAP Global Security

CUSTOMER

THE BEST RUN SAP

Agenda

- Why do we need CVEs and what it is?
- SAP becoming a CNA
- SAP's policy for assigning CVEs
- Understanding the CVE entry from MITRE and NVD
- Why should you care about CVE?
- How you can make use of CVEs to consume SAP patches effectively?

Why do we need CVEs and what it is?

- Problem – each security vendor has its own database with little to no crossover. Each vendor's tool generates its own alert for detected vulnerabilities, and these alerts must be manually cross-referenced between the tools to determine if they are separate issues or multiple alerts for the same issue.

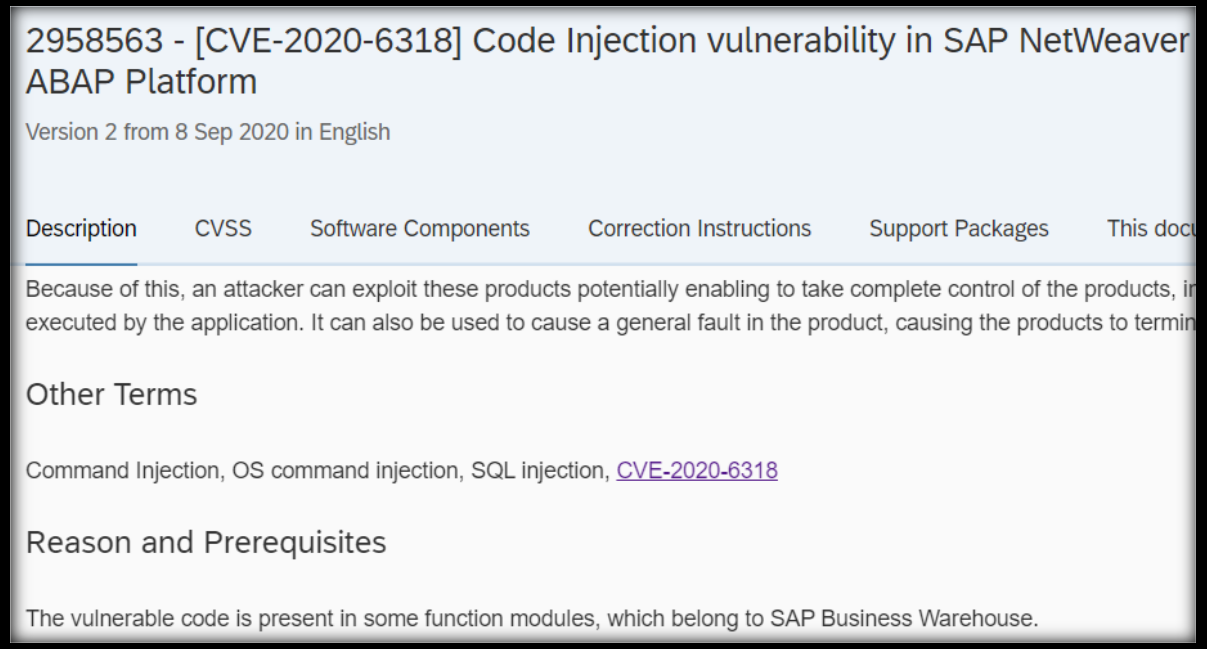
- Starting 1999 CVE IDs were assigned to publicly known vulnerabilities.
  These identifiers make it easy to share information between different databases, tools and services

SAP becoming a CNA

- By becoming a CNA and issuing CVE IDs to security vulnerabilities in SAP products, SAP is able to provide our customers with the inherent benefits of the CVE platform like transparency, automation support and increased patch awareness.
- SAP ensures consistency and authenticity of vulnerability information available in vulnerability databases which are CVE-compatible for vulnerabilities in SAP products.

SAP's policy for assigning CVEs

- All security notes which are released as Patch Day notes get CVE IDs assigned to them from December 2017 patch day.
- CVE IDs are available inside all patch day security notes and you can also get the list of CVEs published on a given Patch Day from our public Patch Day blog



2958563 - [CVE-2020-6318] Code Injection vulnerability in SAP NetWeaver ABAP Platform

Version 2 from 8 Sep 2020 in English

Description | CVSS | Software Components | Correction Instructions | Support Packages | This docu

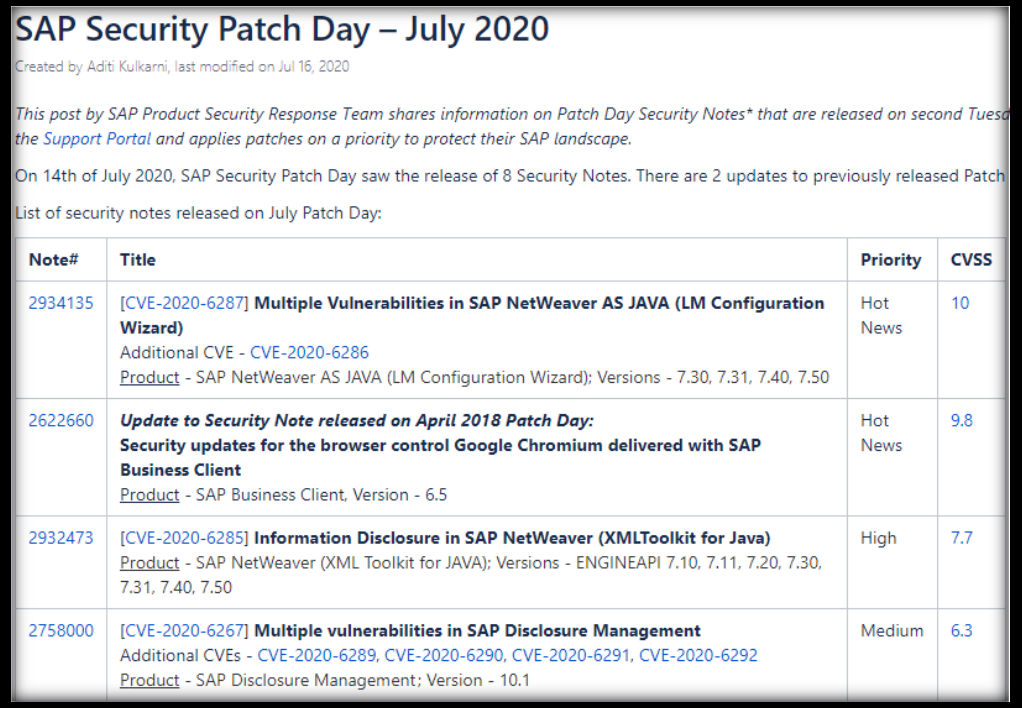
Because of this, an attacker can exploit these products potentially enabling to take complete control of the products, ir executed by the application. It can also be used to cause a general fault in the product, causing the products to termin

Other Terms

Command Injection, OS command injection, SQL injection, CVE-2020-6318

Reason and Prerequisites

The vulnerable code is present in some function modules, which belong to SAP Business Warehouse.



SAP Security Patch Day – July 2020

Created by Aditi Kulkarni, last modified on Jul 16, 2020

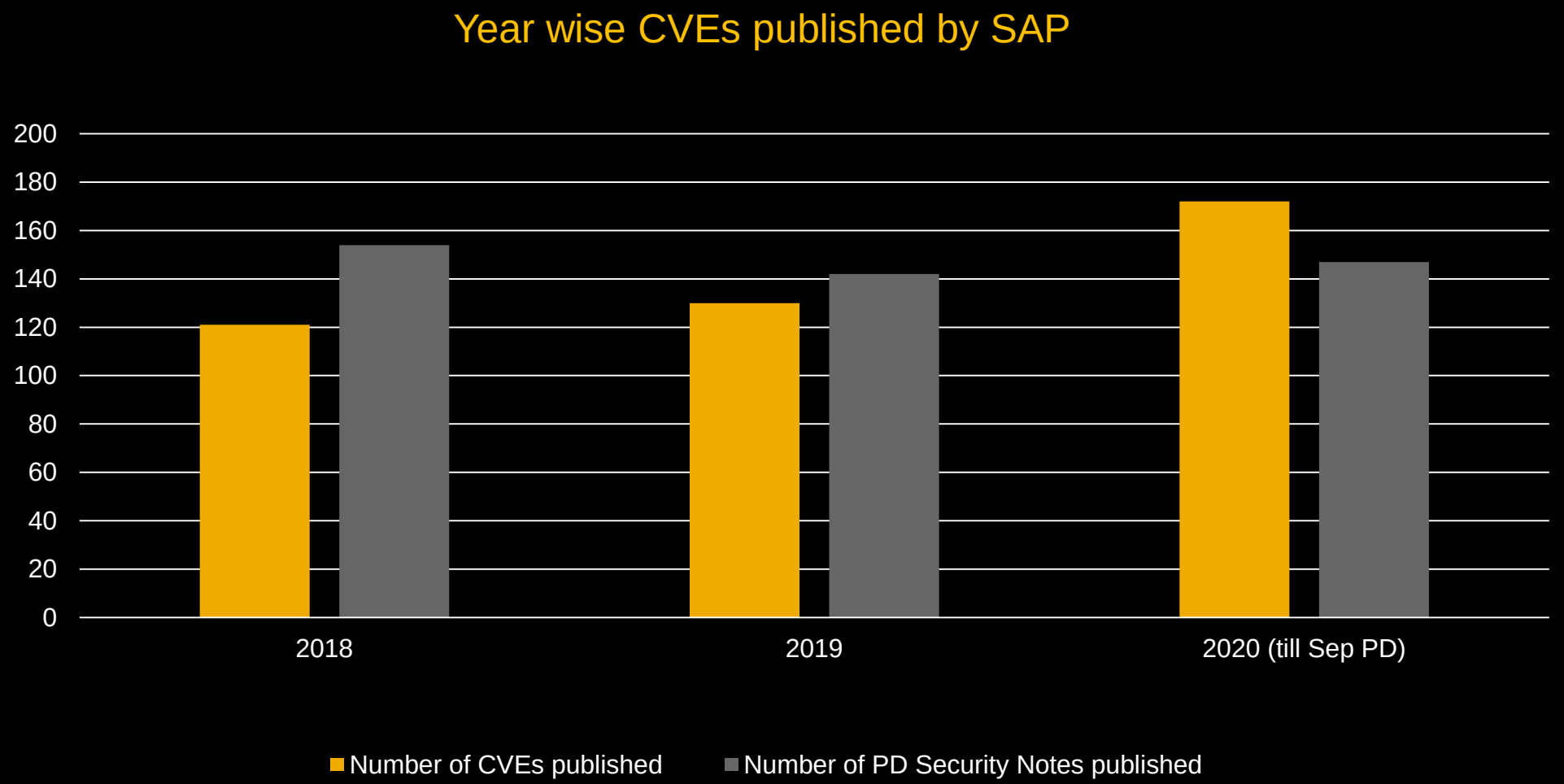
This post by SAP Product Security Response Team shares information on Patch Day Security Notes that are released on second Tuesd the Support Portal and applies patches on a priority to protect their SAP landscape.*

On 14th of July 2020, SAP Security Patch Day saw the release of 8 Security Notes. There are 2 updates to previously released Patch

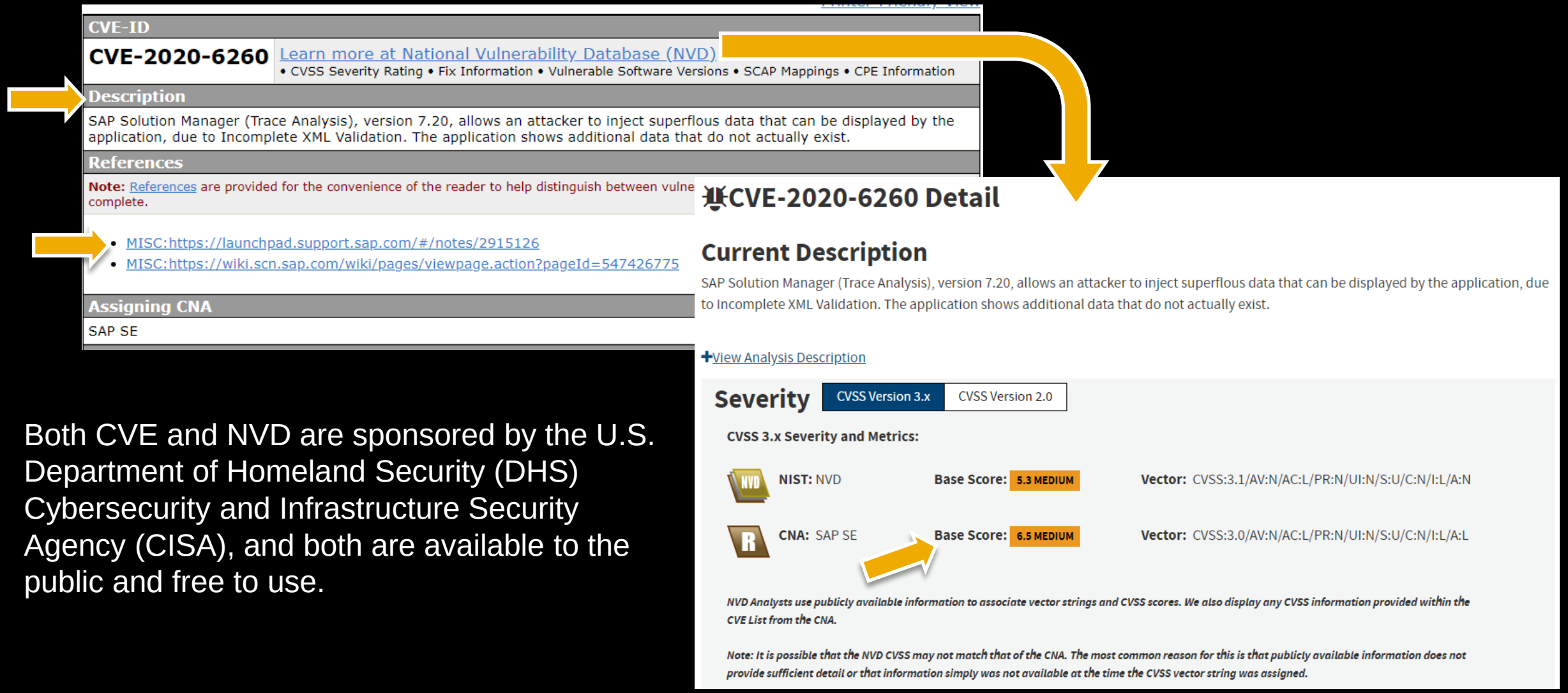
List of security notes released on July Patch Day:

Note#	Title	Priority	CVSS
2934135	[CVE-2020-6287] **Multiple Vulnerabilities in SAP NetWeaver AS JAVA (LM Configuration Wizard)** Additional CVE - CVE-2020-6286 Product - SAP NetWeaver AS JAVA (LM Configuration Wizard); Versions - 7.30, 7.31, 7.40, 7.50	Hot News	10
2622660	***Update to Security Note released on April 2018 Patch Day:*** **Security updates for the browser control Google Chromium delivered with SAP Business Client** Product - SAP Business Client, Version - 6.5	Hot News	9.8
2932473	[CVE-2020-6285] **Information Disclosure in SAP NetWeaver (XMLToolkit for Java)** Product - SAP NetWeaver (XML Toolkit for JAVA); Versions - ENGINEAPI 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	High	7.7
2758000	[CVE-2020-6267] **Multiple vulnerabilities in SAP Disclosure Management** Additional CVEs - CVE-2020-6289, CVE-2020-6290, CVE-2020-6291, CVE-2020-6292 Product - SAP Disclosure Management; Version - 10.1	Medium	6.3

CVEs published by SAP as CNA



Understanding the CVE entry from MITRE and NVD



CVE-ID

CVE-2020-6260 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

SAP Solution Manager (Trace Analysis), version 7.20, allows an attacker to inject superflous data that can be displayed by the application, due to Incomplete XML Validation. The application shows additional data that do not actually exist.

References

Note: References are provided for the convenience of the reader to help distinguish between vulne
complete.

- MISC:https://launchpad.support.sap.com/#/notes/2915126
- MISC:https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=547426775

Assigning CNA

SAP SE

CVE-2020-6260 Detail

Current Description

SAP Solution Manager (Trace Analysis), version 7.20, allows an attacker to inject superflous data that can be displayed by the application, due to Incomplete XML Validation. The application shows additional data that do not actually exist.

+View Analysis Description

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 5.3 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CNA: SAP SE **Base Score:** 6.5 MEDIUM **Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

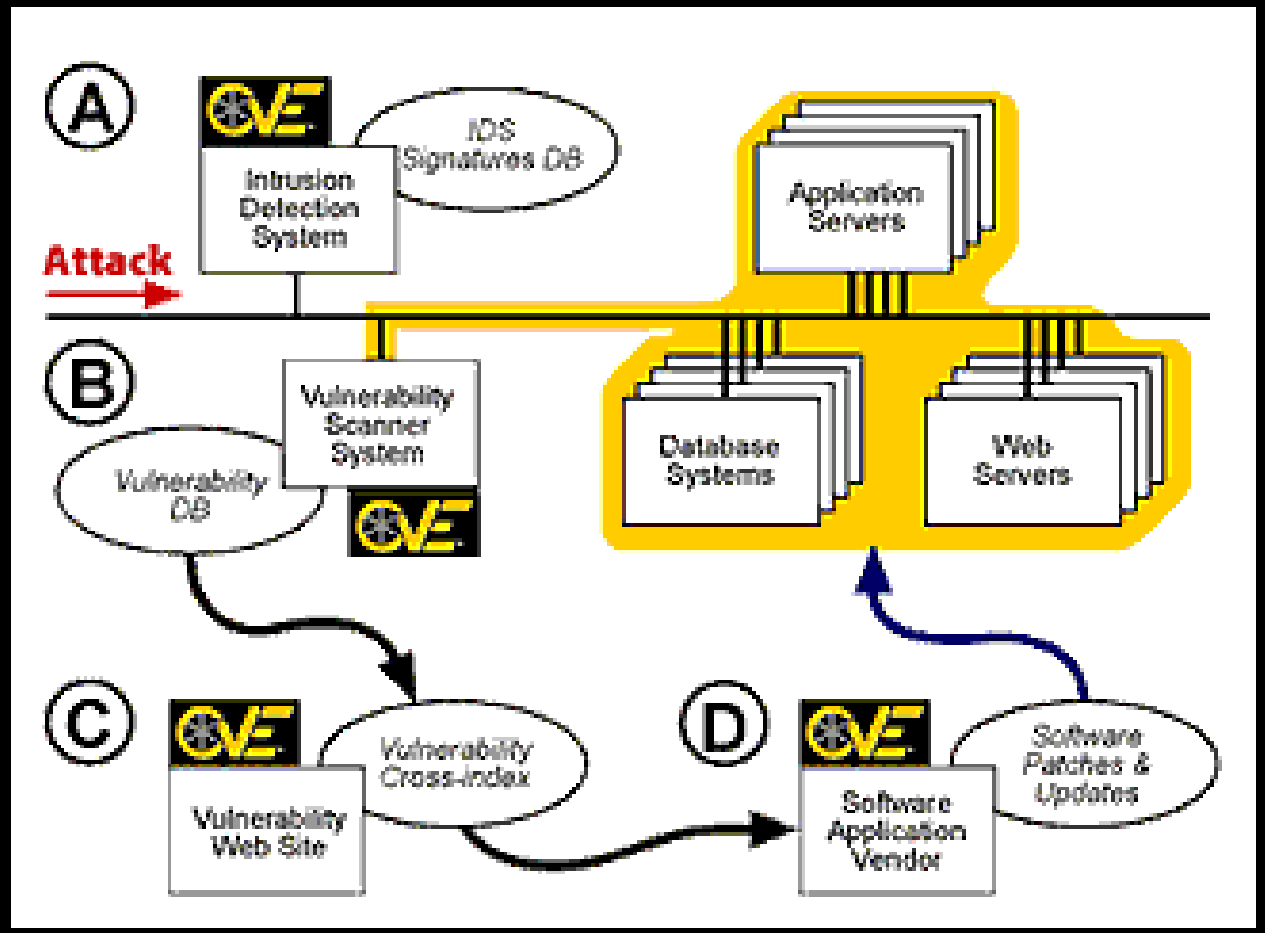
NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: It is possible that the NVD CVSS may not match that of the CNA. The most common reason for this is that publicly available information does not provide sufficient detail or that information simply was not available at the time the CVSS vector string was assigned.

Both CVE and NVD are sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and both are available to the public and free to use.

Why should you care about CVE?

- By using the CVE Identifier for a particular vulnerability or exposure, you will be able to quickly and accurately obtain information from a variety of CVE-Compatible information sources.
- Using CVE-Compatible Products and Services will allow you to improve how your organization responds to security advisories.
- Better search on vulnerabilities and exposures.



How you can make use of CVEs to consume SAP patches effectively

- Understand the limitations of CVE

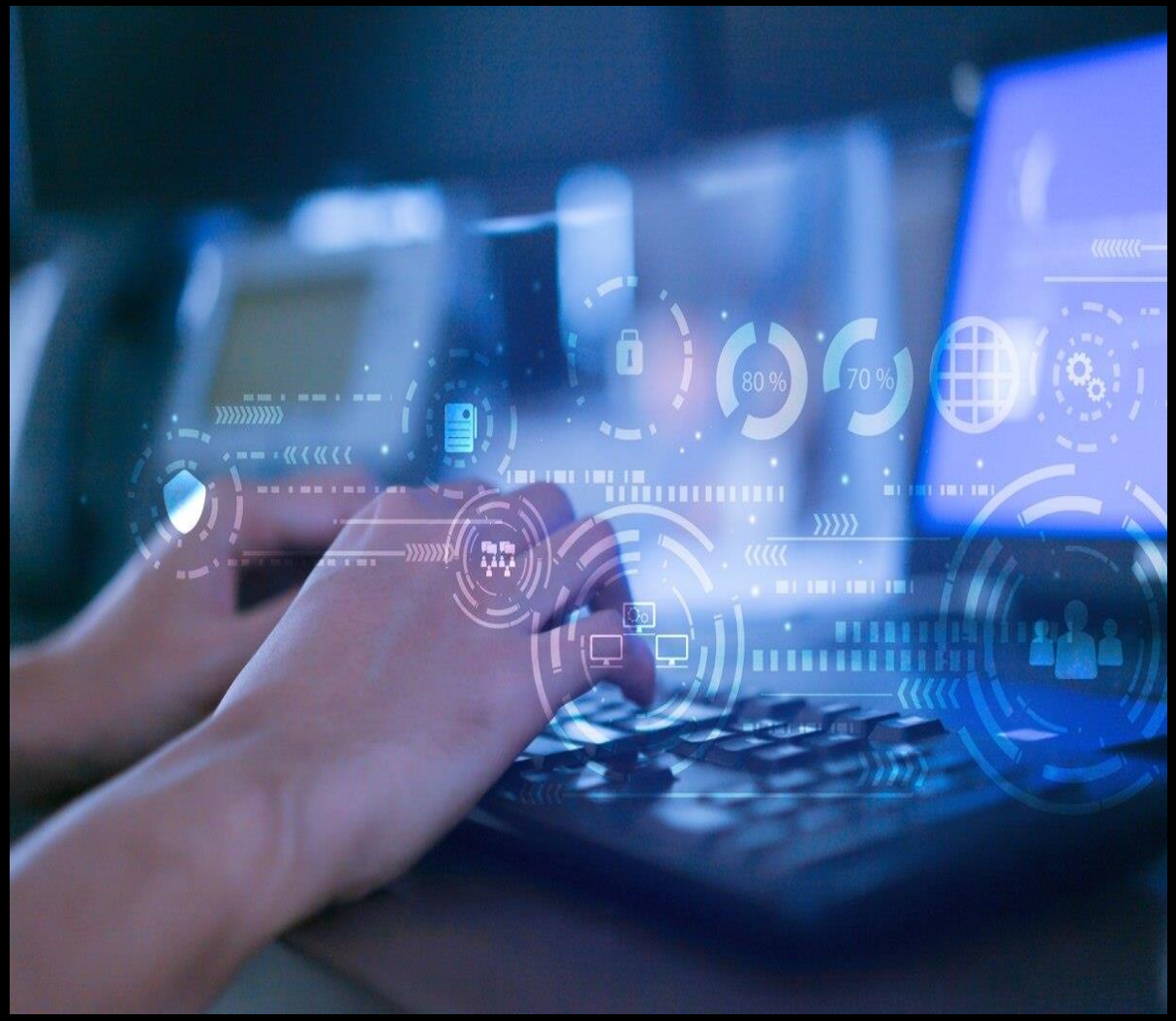
CVE is neither a catch-all nor a cure-all

- Use CVEs to bridge teams

CVEs do form the basis for a common security language. They are easy to understand, to grasp onto.

- Automating CVE prioritization

Leverage third party security partners and automation tools to automatically monitor CVEs related to your specific organization



Resources

https://cve.mitre.org/about/faqs.html

https://cve.mitre.org/compatible/enterprise.html

CVE-Compatible Products and Services

Latest version of the CVE CVE List Master Copy page

A free tool from CERIAS/Purdue University monitors changes to the CVE List

CVE Change Logs provide daily or monthly changes to the list

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SAP

CVE and NVD Relationship

Thank you.

Contact information:

cna@sap.com